International Journal of Computing and Network Technology
ISSN (2210-1519)
Int. J. Com. Net. Tech. 5, No. 3 (Sept.-2017)

http://dx-doi.org/10.12785/ijcnt/050302

Fuzzy Preferences based STRIDE Threat Model for Network Intrusion Detection

Salman A. Khan[1]

[1]*Computer Engineering Department, University of Bahrain, Sakhir, Bahrain*

Received: 25 May 2017, Revised: 18 August: 2017, Accepted: 20 August 2017, Published: (01 September 2017)

Abstract: Security has become a crucial performance measure in today's computer and network systems. One important aspect of this security is to understand the issue as to how different threats could lead to a negative impact and disasters on the functions of a network system. With this consideration, this paper proposes a threat preference approach to evaluate the impact of threats to a system. The proposed approach is synergized with the well-known STRIDE threat model. A tool is also developed to evaluate the level of overall level of overall given a number of threats and threat given a number of threats and threat preference rules. Preliminary analysis of the approach highlights the effectiveness in mitigating threats and attacks.

Keywords: Network Security, Automated decision-making, Fuzzy logic, STRIDE, Fuzzy preferences.

1. INTRODUCTION

Network and data security has become a main pillar of the modern network and computer systems. Due to various network attacks worldwide, a huge amount of money has been lost due to these security breaches and caused damage to assets. Therefore, effective and efficient security systems are needed to protect assets. The purpose of a typical security system is to prevent and detect illegal and unauthorized use of a host (computer) or a network. Thus, a secure network should fulfil the requirements of providing confidentiality, integrity, authentication, non-repudiation, and availability to all valid users [1]. In a well-structured network, a three-level security strategy is adopted [2]:

1. Prevention, where the purpose is to stop an attack from succeeding.
2. Detection, where the purpose is to detect and inform the network administrator if an attack has taken place.
3. Mitigation, which defines the ability to minimize the loss and recovery from an attack.

An important phase during the development of a secure network is to analyze the risk a network could be exposed to. This requires that the threats be identified, in order to ascertain their impact on the asset. In addition, the threat must be identified, and determined as to which aspect of security would be violated by a certain attack. The process of recognizing, measuring, and investigating potential threats of a system is called Threat Modeling [3]. The purpose of threat modelling is to identify the possible threats and rate them according to their level of risk.

Several threat models have been proposed in the literature. One well-known model is the STRIDE model which was proposed by Microsoft [4]. The STRIDE model categorizes threats in a systematic and structured manner. The STRIDE model addresses six main categories of threats which are Spoofing, Tampering, Repudiation, Information disclosure, Denial-of-service, and Elevation of privileges. In [5] and [6], a modified STRIDE model based on the concepts of fuzzy logic was proposed. This paper serves as an extension to the above two studies, and addresses the issue as to how the fuzzy STRIDE model could be modified if the network security administrator intends to assign preferences to certain threat types, compared to others. A preference approach is developed for the STRIDE model which is complemented with a visual tool.

The rest of the paper is organized as follows. Section 2 provides a brief background of the STRIDE model. Section 3 provides the fuzzy preferences based approach for the STRIDE model. This is followed by relevant preferences rules in Section 4. Section 5 discusses the

E-mail: engr.ahmeds@gmail.com

application examples of the proposed approach. Finally, a conclusion is given in Section 6.

2. STRIDE MODEL

The security of any computer and network system is defined with respect to five different categories, as follows [7].

- Integrity - Assuring that data has not been changed illegally
- Availability - Uninterrupted presence of a service or resource
- Confidentiality - Safeguard information from revelation
- Authenticity - Ability to legalize a resource along with data
- Accountability - Skill to confidently relate specific incidents to a particular entity

Considering the aforementioned issues, the STRIDE threat model defines six threat categories [8] which are Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of Privilege. These threat categories help in identifying and dealing with various threats and taking appropriate steps to prevent, detect, and mitigate various attacks. Below, details of each threat in the STRIDE model are briefly discussed. A detailed discussion can be found in [5].

Spoofing or "Identity spoofing" refers to a scenario where a user A pretends to be a user B by changing his identity and gains illegal access to protected data. This may result in vulnerabilities, which makes it necessary to authenticate the user's identity. *Tampering* refers to change of data by an unauthorized person who is not allowed to modify the data. If packets sent by a user over a network are tampered with, it would affect the integrity of the system [4]. Thus, the integrity can be maintained by blocking an unaccredited user from manipulating the data. *Repudiation* depends on the notion that a security system must always be able to trace the entity responsible for any illegitimate modification and illegal access of resource or account. This is known as the non-repudiating act of any network. *Information Disclosure* enables an attacker or malicious user to access confidential information. Users are fairly cautious about submitting private details to a system or other user through a network. *Denial of Service* attack is an attempt to disturb a resource, network, or system in such a way that the intended and valid user would not be able to use it. In *Elevation of Privilege* attack, the intruder gets a higher level of authorization than what had originally been granted [9].

3. FUZZY LOGIC BASED PREFERENCE APPORACH FOR STRIDE THREAT MODEL

Fuzzy logic was originally proposed by Lotfi Zadeh in 1965 [10] and since then has been successfully applied to a range of problems such as analog circuit design [11], war resource allocation [12], direct current electromagnetic design [13], and facility location selection [14], among many others.

An important application of fuzzy logic is in the domain of multi-criteria decision making (MCDM) which deals with automated decisions in the presence of multiple and conflicting criteria. In such problems, the aim is to find the best solution from a set of feasible solutions. The fuzzy logic based MCDM approach requires that the different criteria, which generally differ from each other in terms of magnitude and units, are combined into a single decision function. This methodology is known as "scalarization" where the final decision is measured based on a value on a scale of 0 to 1. A value near 1 suggests a near optimal solution while a value near 0 indicates an inefficient solution.

In [5] and [6], a fuzzy logic based STRIDE model was proposed. The following decision rule was used.

Rule 1: "IF spoofing is low AND tampering is low AND repudiation is low AND information disclosure is low AND denial of service is low AND elevation of privilege is low then the attack is low"

The above rule indicates the conditions in which different attacks are supposed to be detected.

The Unified and-Or (UAO) operator, proposed by Khan and Engelbrecht [15], behaves as a soft-And or soft-Or operator. The primary feature of the operator is that a single equation is used to represent the soft-AND function or the soft-OR function. The behavior of the operator is controlled by a variable $\nu \geq 0$, whose value decides whether the function behaves as soft-AND or soft-OR. The operator is defined as

$$f(a,b)=\frac{ab+\nu\max\{a,b\}}{\nu+\max\{a,b\}}=\begin{cases}\mathrm{I}_{\star}=\mu_{A\cup B}(x) & \text{if } \nu>1\\ \mathrm{I}^{*}=\mu_{A\cap B}(x) & \text{if } \nu<1\end{cases}$$

where 'a' represents the membership value of first decision criteria, 'b' represents the membership value for second decision criteria and f (a, b) represents the value of the overall objective. I^{*} represents the soft-AND operation using the UAO operator, and I_{*} denotes the soft-OR operation using the UAO operator. With $0 < \nu < 1$, the behavior of UAO is soft-AND, whereas a value of $\nu = 0$ gives the pure-AND behavior of Zadeh's MIN function.

With regard to Rule 1, the Unified And-Or operator can be mathematically written as follows

$$f(x)=\frac{\mu_S\mu_T\mu_R\mu_I\mu_D\mu_E+\nu.\max\{\mu_S,\mu_T,\mu_R,\mu_I,\mu_D,\mu_E\}}{\nu+\max\{\mu_S,\mu_T,\mu_R,\mu_I,\mu_D,\mu_E\}} \quad (7)$$

In the above equation, f(x) represents the overall decision function. This overall decision function signifies the level of attack on the network. Note that the value of f(x) is in the range of [0,1]. The nearer the value of f(x) to 1, the higher is the level of attack, whereas a low value of f(x) indicates a low level of attack.

One limitation of the above rule is that it treats all attacks with the same preference. However, in real systems, there might be situations in which the network security administrator would like to give more consideration to one (or more) decision criteria (i.e. attacks). This scenario motivates the use of preference based rules in order to provide flexibility to the fuzzy STRIDE model. For this purpose, the preference scheme proposed in [15] is employed. The scheme has 7 levels of preferences and therefore can model preferences to a sufficient level of granularity. The scheme is given in Figure 1.

The evaluation values can be seen as consisting of two groups: 1) s_i preferred to s_j and 2) s_j preferred to s_i. Here, s_i and s_j represent two optimization objectives. It is realized that the two groups are similar and equivalent since, if the first objective is preferred to the second, then the second objective is not preferred to the first. This approach uses values between 0 and 1, which make it simple and easy to use with fuzzy logic, and consists of seven terms.

$$\mu(s_i,s_j)=\begin{cases}1 & \text{if } s_i \text{ is definitely preferred to } s_j\\ c\in(0.916,0.999) & \text{if } s_i \text{ is strongly preferred to } s_j\\ d\in(0.832,0.915) & \text{if } s_i \text{ highly preferred to } s_j\\ e\in(0.748,0.831) & \text{if } s_i \text{ is considerably preferred to } s_j\\ f\in(0664,0.747) & \text{if } s_i \text{ is moderately preferred to } s_j\\ g\in(058,0.663) & \text{if } s_i \text{ is slightly preferred to } s_j\\ h\in(501,0.579) & \text{if } s_i \text{ is mildly preferred to } s_j\\ 0.5 & \text{if there is no preference}\\ i\in(0.421,0.499) & \textit{if } s_j \textit{ is mildly preferred to } s_i\\ j\in(0.337,0.42) & \text{if } s_j \text{ is slightly preferred to } s_i\\ k\in(0.253,0.336) & \text{if } s_j \text{ is moderately preferred to } s_i\\ l\in(0.169,0.252) & \text{if } s_j \text{ is considerably preferred to } s_i\\ m\in(0.085,0.168) & \text{if } s_j \text{ is highly preferred to } s_i\\ n\in(0.001,0.083) & \text{if } s_j \text{ is strongly preferred to } s_i\\ 0 & \text{if } s_j \text{ is definitely preferred to } s_i\end{cases}$$

FIGURE 1: THE ADOPTED PREFERENCE SCHEME

4. PREFERENCE RULES FOR MULTI-CRITERIA STIRDE INTRUSION DETECTION

The preference terms defined in the previous section can be utilized to define various preference rules. These rules are divided into several categories, as described below.

A. Preference rules involving all six objectives

A number of preference rules can be developed under this category. Some examples of such preference rules are as follows

- PR1a: Spoofing is strongly preferred over the other five objectives.
- PR1b: Tampering is highly preferred over the other five objectives.
- PR1c: Repudiation is strongly preferred over the other five objectives.
- PR1d: Information Disclosure is slightly preferred over the other five objectives.
- PR1e: Denial of Service is slightly preferred over the other five objectives.
- PR1f: Elevation of Privileges is mildly preferred over the other five objectives.

B. Preference rules involving five objectives

Some possible rules are as follows.

- PR2a: Denial of Service is strongly preferred over Tampering, Repudiation, Spoofing, and Information Disclosure.
- PR2b: Information disclosure is highly preferred over Tampering, Repudiation, Spoofing, and Elevation of Privileges
- PR2c: Spoofing is slightly preferred over Tampering, Repudiation, Denial of Service, and Information Disclosure.
- PR2d: Tampering is slightly preferred over Spoofing, Repudiation, Denial of Service, and Information Disclosure.

C. Preference rules involving four objectives

Some possible rules are as follows.

- PR3a: Repudiation is strongly preferred over Tampering, Spoofing, and Elevation of privileges.
- PR3b: Spoofing is considerably preferred over Information Disclosure, Elevation of privileges, Tampering, and Repudiation.
- PR3c: Tampering is mildly preferred over Spoofing, Repudiation, and Information Disclosure.
- PR3d: Denial of Service is considerably preferred over Spoofing, Repudiation, and Tampering.

D. Preference rules involving three objectives

Some possible rules involving three objectives could be as follows.

- PR4a: Denial of service is moderately preferred Information disclosure and Tampering
- PR4b: Elevation of privileges is considerably preferred over Elevation of privileges and Repudiation.

- PR4c: Tampering is strongly preferred over Spoofing and Repudiation.
- PR4d: Repudiation is highly preferred over Spoofing and Information Disclosure.

E. Preference rules involving two objectives

Some rules involving two objectives could be formed as follows.

- PR5a: Information disclosure is slightly preferred over Tampering
- PR5b: Repudiation is highly preferred over Elevation of privileges.
- PR5c: Spoofing is highly preferred over Elevation of Privileges
- PR5c: Tampering is definitely preferred over Repudiation

F. Interpretation of decision rules

Based on the preference rules, the final step is the evaluation of the threat level based on the threat preference rules. In this study, three threat levels are defined which are 'Low', 'Moderate' and 'High' as follows.

For $0 < f(x) < 0.3$ the threat level is 'Low'

For $0.3 \leq f(x) \leq 0.5$ the threat level is 'Moderate'

For $f(x) > 0.5$ the threat level is 'High'

Note that these levels are flexible and can be adjusted by the security administrator as desired.

5. RESULTS

A prototype tool consisting of ten different rules was developed. The tool is flexible in terms of adding or deleting rules, and the security administrator has control of the tool in terms of defining the rules. Figures 2 and 3 show two instances of threat level detection using the tool. In Figure 2, preference rule PR2b is assessed. The corresponding values of different threats and their count are given. Based on these values, the system generates the overall threat level of 0.258 which corresponds to attack level as "Low".

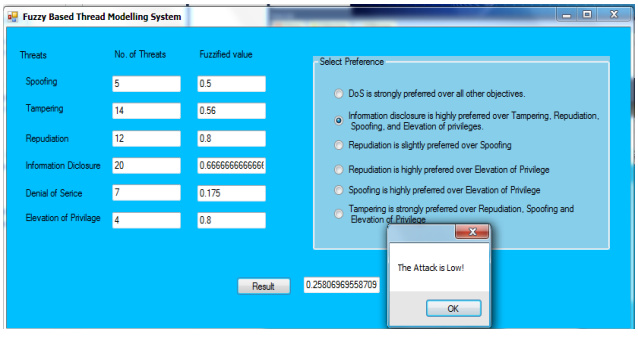

FIGURE 2: EVALUATION OF PREFERENCE RULE PR2B

Similarly, Figure 3 shows the evaluation of preference rule PR5c. The output value is 0.310 which corresponds to a level of "Moderate".

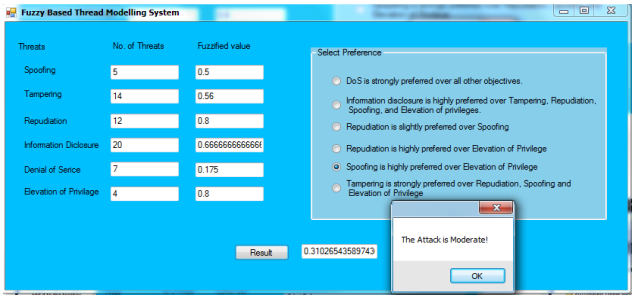

FIGURE 3: EVALUATION OF PREFERENCE RULE PR5C

6. CONCLUSION

This work proposed a STRIDE based threat modeling scheme by incorporating user preferences in the decision process through the use of fuzzy logic. A tool was developed which takes the preference rule and attack values as inputs and evaluates the level of the threat accordingly as low, moderate, or high. Preliminary analysis suggest that the proposed approach satisfactorily deals with the issues of measuring impact of simultaneous attacks, with preference given to one or more specific attacks.

The work proposed in this paper can be extended in several directions. One direction is to apply the proposed approach to other threat models such as DREAD, SWOT, and OWASP. Another direction is to use other preference approaches proposed in literature and compared to the one used in this paper.

ACKNOWLEDGMENT

The author thanks the Deanship of Scientific Research at University of Bahrain for supporting this work under Project # 24/2015. The author also acknowledges the assistance provided by Mr. Faiz Iqbal.

REFERENCES

[1] The STRIDE Threat Model, http://msdn.microsoft.com/enus/library/ee823878%28v=cs.20%29.aspx, 2002

[2] M. Curtin, Introduction to Network Security, Kent Information Services, Inc., March 1997.

[3] A. S. Sodiya, S. A. Onashoga and B. A. Oladunjoye, Threat Modeling using Fuzzy Logic Paradigm, Volume 4, 2007

[4] A. Shostack, S. Lambert, S. Hernan, Uncover Security Design Flaws using STRIDE, MSDN magazine, November 2006.

[5] S. A. Khan, A STRIDE Model based Threat Modelling using Unified and-Or Fuzzy Operator for Computer Network Security, International Journal of Computing and Network Technology, 5(1) 13-20, January 2017.

[6] S. A. Khan, Fuzzy STRIDE Model based on Werners Aggregation Operator for Computer Network Threat Modelling, International Journal of Computing and Digital Systems, 6(2) 83-88, March 2017.

[7] W. Stalling, L. Brown, Computer Security: Principles and Practice, 2nd edition, Pearson Education, 2008.

[8] B. Daya, Network Security: History, Importance, and Future, University of Florida.

[9] M. A. Anton, J. M. Barnes, STRIDE-based Security model, Institute of software research, January 2010.

[10] J. Kacprzyk, M. Fedrizzi, H. Nurmi, Group decision making and consensus under fuzzy preferences and fuzzy majority, Fuzzy Sets and Systems 49, 21–31, 1992.

[11] G. Oltean, C Miron, and E. Moccan. Multiobjective Optimization for Analog Circuits Design based on Fuzzy Logic. In 9th International Conference on Electronics, Circuits and Systems, pages 777 – 780, 2002.

[12] S. Palaniappan, S. Zein-Sabatto, and A. Sekmen. Dynamic Multiobjective Optimization of War Resource Allocation using Adaptive Genetic Algorithms. In IEEE SoutheastCon, pages 160 – 165, 2001.

[13] M. Chiampi, C. Ragusa, and M. Repetto. Fuzzy Approach for Multiobjective Optimization in Magnetics. IEEE Transactions on Magnetics, 32(3):1234 – 1237, 1996.

[14] C. Kahraman, D. Ruan, and I. Doan. Fuzzy Group Decision-making for Facility Location Selection. Information Sciences, 157:135–153, 2003.

[15] S. A. Khan and A. P. Engelbrecht. A new fuzzy operator and its application to topology design of distributed local area networks. Information Sciences, 177(13), pp.2692-2711, 2007.

Salman A. Khan received his Ph.D. in computer science from the University of Pretoria, South Africa in 2009. He is currently an Assistant Professor of Computer Engineering at the University of Bahrain. He has over 50 publications in reputed journals and conferences. His research areas are evolutionary computation, fuzzy logic optimization, network design and optimization, and network security.